Support plan

Dr Nikolaos Papas and Fredrik Cornell give a status report on SUPPORT, the EC-sponsored project which aims to help increase port security and improve trade flow

Dr Nikolaos Papas is a Senior Consultant with BMT Hi-Q Sigma Ltd. Fredrik Cornell is Strategic Development Director with Securitas Services Europe.

The *Security UPgrade for PORTs* (*SUPPORT*) project will issue periodic updates on its progress, which can be tracked at: www.support-project.eu.

If you wish to provide feedback or gain further information, please email: supportproject@bmtproject.net.

The **European Commission** (**EC**) has commissioned a project called *Security UPgrade for PORTs* (*SUPPORT*) with the ambitious aim of improving port security in major and minor European ports, whilst at the same time improving the trade flow through these ports as well.

The SUPPORT project, which was presented at the *ASIS International 10th European Security Conference & Exhibition* which took place on 3-6 April in Vienna, receives funding under the Seventh Framework Programme for Research and Technological Development, and is led by an experienced consortium of 19 companies from across the European Union (EU).

European port security is high on the agenda in Brussels, but following the mixed results of the introduction of the *International Ship and Port Facility Security (ISPS) Code* and *EC Legislation 725/2004*, more work remains to be done. Briefly, the key issues that must be tackled for European port security to be increased effectively are:

- no central body for port security
- lack of awareness amongst terminal operators
- lack of international standards for training and security equipment.

Why and how are the above points reducing European port security effectiveness?

The European Union consists of 27 member states, 22 of which are flag states. One of the cornerstone principles of the EU is the Principle of Subsidiarity, the belief and ultimate respect for national sovereignty that ensures the member states largely govern themselves in the manner that best befits their own individual needs. It means that Brussels will rarely, if ever, get involved in 'low-level' national matters, such as mandating how administrations are organised and legislation is implemented.

In fact, Article 5(3) of the Treaty on European Union states that: 'The Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States…but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.' This shows how Brussels will try to keep interference in national matters to a minimum. How is this related to port security?

'There is no European-wide appreciation and handling of port security matters. There is no European Department of Homeland Security'

Port security, as a concept, is treated differently in different European flag states. In some countries, port security is provided by a combination of military and police forces. In other countries, it is a completely commercial arrangement where private enterprises hire private security companies to provide port security. In other words, there is no European-wide appreciation and handling of port security matters. There is no European Department of Homeland Security.

There are some European bodies that touch upon subjects of port security. The **European Maritime Safety Agency** (**EMSA**) is a European body advising on maritime safety issues. **FRONTEX** is a European body advising and assisting in border control issues. **EUROPOL** can be an asset in combating organised crime. However, the big drawback of these organisations is that they have no executive powers and cannot control national operations. A EUROPOL officer cannot arrest a suspect in a member state; he has to request assistance from a national police force.

There are, therefore, two important issues here. Firstly, a European body that concerns itself exclusively with port security does not exist. Secondly, even if it did, it would have no executive powers and therefore a 'European' approach to port security would still not be viable.

This leads to the second issue: the terminal operators. Due to the above,

port security has been devolved to terminal operators. Terminal operators are, for the most part, private enterprises that obey two primary authorities: their shareholders and their Executive Board. These two authorities have only one combined aim: make profits. Herein lies a dilemma – port security investments have always been seen as a 'necessary nuisance', a cost that reduces profits through the necessary investments and through the barriers it puts up in the flow of goods through ports. Whilst there are some ports that have embraced the **International Organization for Standardization's** *ISO 28000* and similar initiatives and see security investments as an opportunity and not a burden, the majority of ports in the EU simply do not have the luxury to invest in such lavish security management systems. The introduction of the ISPS Code has cost billions of dollars around the world, for little perceived benefit – and terminal operators and ports remember these mandated investments with some scorn.

Low-priority issue

This problem is exacerbated by the fact that the majority of ports see security as a low-priority issue. They believe that there is a low to non-existent terror threat against ports, and they often seem to think that matters of terrorism are dealt with by police and the military. Furthermore, many maintain that matters of crime do not affect them directly either. In other words, terminal operators are in many cases reluctant to invest money in security measures that do not directly protect their income from a direct and perceived threat. Nor are terminal operators and ports willing to acknowledge a real and direct threat from terrorism.

This leads on to the final issue: the lack of standards. When the ISPS Code was introduced, the legislation did not mandate specific security measures and how to implement them. There were no requirements for fence quality (in fact, fences themselves were not mandated), there were no requirements for security patrols, there were no advocated minimum standards for security qualifications and training, and so forth.

This lack of detail in the legislation has led to a situation where there are vast differences within the EU in how the ISPS Code is implemented. For example, whilst some ports have interpreted the ISPS Code requirements for protected facilities in such a way that they require the use of code cards, fences, closed circuit television (CCTV) and alert systems, other ports have interpreted that a yellow line around the terminal boundary is sufficient to be in compliance. Clearly, this is a very unsatisfactory state of affairs.

Challenging domain

It is within this challenging domain that SUPPORT aims to effect change that will increase port security in the EU. The SUPPORT project will tackle this problem from a multitude of angles.

Firstly, SUPPORT will study existing legislation and identify draw-backs, gaps and ambiguities. Using structured approaches, such as ISO 28000, and security initiatives such as CSI, C-TPAT, AEO, etc., we will propose amendments to legislation that will provide clearer guidance to actors in the logistics supply chain on how to improve their port security. Where relevant, we may also propose changes to existing public bodies, to take a more pro-active role in the enforcement of security standards.

Secondly, SUPPORT will undertake a detailed study that will:

- analyse the current threats from crime and terror
- identify the most important and effective security measures that can effectively reduce the threats.

This detailed study will achieve two major aims:

- port actors will be made aware of threats, their probability and their precise potential for disruption
- port actors will be given an interactive tool that can show cost versus effectiveness for specific threats.

Investment for business

Considering the feedback we have received so far, these aims will be important in making ports aware that investment in security measures is not money thrown away, but rather an investment for business continuity. We have received strong interest in our ongoing analysis of tying down the investment cost of particular security measures, versus its impact on the flow of goods through a port, versus its effectiveness against different threat scenarios (crime and terrorism). We surmise this is because past investments in security measures have not shown any real cost-benefit. Our method will show an explicit link between flow, cost and effectiveness, and provide ports with decision tools that do not exist.

Finally, SUPPORT will develop a suite of solutions for upgrading port security. These solutions will:

- not impede, but accelerate, the flow of goods through ports
- be modular, so ports and terminal operators can 'plug and play' solutions that are most pertinent for their own unique situations
- be scalable, so they can be affordable from the smallest single-quay ports to the largest megaports.

These solutions will be designed in such a way that the latest advances in technology and legislation are accounted for, will be accompanied with plenty of explanatory material highlighting whether, how, when and where to deploy each solution and guidance on the cost and effectiveness side.

The solutions will be comprised of:

- best practice-based processes and procedures for patrolling, checking, scanning, incident management, etc.
- a port security training programme, based on worldwide experiences
- software solutions providing advanced data fusion and decision support capabilities
- standards for security 'hardware': e.g. fence heights, CCTV coverage, etc.

The four-year SUPPORT project will develop these solutions in years two and three, and will then run a number of full-scale pilot cases in a number of European ports where the validity and applicability of the SUPPORT solutions will be tested and demonstrated.